ABSTRACT OF THE DISCLOSURE

An object of this invention is to eliminate the necessity to manage a plurality of keys even when image data having a plurality of tiles and layers is

5 encrypted using different encryption keys for the respective tiles and layers. For this purpose, in this invention, a code stream c compression-coded for each tile is received. In repeatedly forming one tile group from a plurality of adjacent tiles and another tile

10 group from adjacent tile groups to define the hierarchical structure of the tile groups, an encryption tile part designation section determines which tile group in which layer should be encrypted and outputs encryption tile information ta. A key matrix

15 generation section (12) generates an encryption key ck for the whole of the received code stream c, sequentially generates the encryption key of each node in the hierarchical structure, and outputs the result as a key matrix ka. An encryption section (13)

20 encrypts a tile to be encrypted by using the key generated for that tile and outputs an encrypted code stream c'.